Greenbaum
Law Group, LLP

3 Columbus Circle, Suite 1500
New York, New York 10019
Tel: (949)-760-1400

Honorable Edgardo Ramos
United States District Court, Southern District of New York
Thurgood Marshall United States Courthouse
40 Foley Square
New York, NY 10007

July 21, 2025

RE: *Nelson Estrada v. TaskUs, Inc.*, No. 1:25-cv-04409

Dear Judge Ramos:

I write on behalf of Plaintiff Nelson Estrada in response to Defendant TaskUs, Inc.'s ("TaskUs") request to file a motion to dismiss. TaskUs's letter relies on inapposite case law and is directly contradicted by its own public statements and securities filings. For the reasons below, TaskUs's anticipated motion to dismiss should be denied.

Brief Factual Background: Mr. Estrada's complaint asserts that TaskUs is liable for failing to prevent its employees from selling Mr. Estrada and others' personally identifiable information to cyber criminals, including customer names and contact information, as well as social security numbers, bank account identifiers, and transaction data. This highly sensitive data was entrusted to TaskUs by Coinbase, Inc. ("Coinbase"), a cryptocurrency exchange, and by Mr. Estrada and the class of Coinbase customers he seeks to represent. The results of TaskUs's failure have been catastrophic: Coinbase estimates customers have lost $400 million to criminals working with TaskUs employees.

Mr. Estrada's Complaint Alleges Significant Injuries: TaskUs' July 17 Letter argues that the Complaint does not allege an injury-in-fact. The argument is specious given the magnitude of stolen funds at issue: $400 million. And unsurprisingly, TaskUs fails to cite the governing standard for alleging injuries in the data breach context. In *McMorris* v. *Carlos Lopez & Assoc., LLC*, the Second Circuit held that in a data breach case courts should consider, "whether the plaintiffs' data has been exposed as a result of a targeted attempt to obtain that data," whether "the dataset has already been misused," and whether the exposed data is "sensitive." 995 F.3d 295 (2d Cir. 2021). All of these factors are present here. Mr. Estrada's complaint alleges Coinbase notified him that his data had been "improperly accessed," Compl. ¶ 15, that criminals used that data to steal up to $400 million in cryptocurrency assets, Compl. ¶ 12, and that the exposed data was highly sensitive, including bank account information. Compl. ¶ 1. TaskUs' citation to inapposite medical monitoring cases should be rejected out of hand.

TaskUs Owed a Duty to Mr. Estrada: TaskUs's next arguments fare even worse. Citing an unpublished district court case from 2010, TaskUs argues that it did not owe Mr. Estrada a duty of care because Mr. Estrada "had no relationship with TaskUs." July 17 Letter at 2 (citing *Hammond v. Bank of N.Y. Mellon Corp.,* 2010 WL 2643307, at *9 (S.D.N.Y. 2010)). This exact argument

Greenbaum
Law Group, LLP

3 Columbus Circle, Suite 1500
New York, New York 10019
Tel: (949)-760-1400

has been roundly and consistently rejected. *See, e.g. Toretto v. Donnelly Fins. Sols., Inc.* 583 F. Supp. 3d 570, 594 (S.D.N.Y. 2022) (rejecting *Hammond* as out-of-date and citing numerous cases denying motions to dismiss advanced by third party service providers in the data breach context); *see also In re GE/CBPS Data Breach Litig.,* 2021 U.S. Dist. LEXIS 146020, at *2 (S.D.N.Y. Aug. 4, 2021) (employees of General Electric properly alleged negligence claims against General Electric's document management company); *In re Experian Data Breach Litig*., 2016 U.S. Dist. LEXIS 184500, at *1 (C.D. Cal. Dec. 29, 2016) (customers of T-Mobile properly alleged negligence claims against third party data server owner that contracted with T-Mobile).

Indeed, in a public filing TaskUs itself has acknowledged obligations to its customer's customers. Its most recent annual report stated that in the event of a data security incident, it "may be subject to claims of liability by [its] clients ***or their customers*** based on the misconduct or malfeasance of our employees." Task-Us, Inc., Annual Report (Form 10-K) (filed Feb. 10, 2025), at 16, *available at* https://ir.taskus.com/static-files/8e218043-c18d-40cb-9958-e034696fecb0.

TaskUs's next argument—that Mr. Estrada "cannot plausibly link TaskUs to the alleged theft of his data"—is directly contrary to their own public statements. In response to Mr. Estrada's complaint, a TaskUs spokesperson told Bloomberg that it had "identified two individuals who illegally accessed information from one of our clients . . . We immediately reported this activity to the client, terminated the individuals involved, and are coordinating with law enforcement." Bloomberg, *Coinbase Customer Service Provider Sued Over Data Breach* (May 28, 2025), *available at* https://news.bloomberglaw.com/litigation/taskus-employees-responsible-for-coinbase-data-breach-suit-says. Contrary to TaskUs's argument, there is far more than a "mere temporal connection" between TaskUs and the Coinbase data breach. As Mr. Estrada alleges in his complaint, "[t]hose involved in the termination [of TaskUs employees] have stated that the fraud pertained to TaskUs' provision of support services to Coinbase." Compl. ¶ 26. TaskUs' contradictory position does not provide grounds to seek to dismiss Mr. Estrada's complaint.

Remaining Claims: Plaintiff's complaint states viable causes of action for the remaining claims as well.

- **Negligence per se.** While there is a split in authority concerning whether Section 5 of the FTC Act may support a negligence per se claim, several courts have upheld them. *See, e.g. In re Capital One Consumer Data Sec. Breach Litig.,* 488 F. Supp. 3d 374, 407-08 (E.D. Va. 2020) (holding that New York law would permit plaintiffs to assert a negligence per se claim premised on Section 5 of the FTCA). TaskUs cites no contrary authority that is published, much less binding.

- **Breach of Implied Contract:** Estrada sufficiently alleges that he provided his personal information to Coinbase and thus to its service providers like TaskUs under an implied contract to keep that personal information safe and secure. *See Lazar* v. *Int'l Shoppes, LLC,* 2025 U.S. Dist. LEXIS 98054, at *9 (E.D.N.Y. May 22, 2025) ("Employees and customers were required to provide their PII and PHI to defendants in exchange for

Greenbaum
Law Group, LLP

3 Columbus Circle, Suite 1500
New York, New York 10019
Tel: (949)-760-1400

employment, products, or services and "reasonably understood that a portion of the funds they paid . . . would be used to pay for adequate cybersecurity measures.").

- **Unjust Enrichment:** Estrada properly alleges that he conferred a benefit on TaskUs through his payments to Coinbase, which in turn paid TaskUs for its services. *See, e.g., In re Ambry Genetics Data Breach Litig.*, 567 F. Supp. 3d 1130, 1145 (C.D. Cal. 2021) (unjust enrichment claim survived motion to dismiss where "Plaintiffs alleged that they paid Defendants money for Defendants' services and expected that a portion of their payments would go toward 'data management and security.'").

- **Declaratory and Injunctive Relief:** A pleadings-based dismissal of claims for declaratory and injunctive relief is inappropriate. *See, e.g., In re Ambry Genetics Data Breach Litig.,* 567 F. Supp. 3d 1130, 1151 (C.D. Cal. 2021) (denying motion to dismiss "Plaintiffs' final claim in their SAC [] for 'Injunctive and Declaratory Relief'"). Moreover, Estrada is not asserting a standalone claim for declaratory and injunctive relief, but rather asserts a claim under the Federal Declaratory Judgment Act. Compl. ¶ 131. The authority cited by TaskUs is inapposite, as it concerns the dismissal of claims for injunctive relief premised on N.Y. GBL § 349 where the plaintiff had not pleaded viable claims under the statute. *See Chiste v. Hotels.com L.P.*, 756 F. Supp. 2d 382, 407 (S.D.N.Y. 2010).

- **Unfair Competition Laws:** Estrada's complaint includes numerous detailed allegations demonstrating that TaskUs's security failures breach FTC regulations and the FTC Act. As those obligations are coterminous with state law unfair competition laws, Estrada's claims under those statutes must survive.

- **California Consumer Privacy Act (CCPA):** The CCPA provides that "[i]n the event a cure is possible," a company can avoid liability if it "actually cures" the violations within 30 days. Ca. Civ. Code 1798.150(b). Here, because TaskUs's employees sold Mr. Estrada's and others' personal information to criminals who utilized that data to steal $400 million in cryptocurrency assets, TaskUs's violations cannot be cured and thus notice is not required. TaskUs's arguments about extraterritoriality are also incorrect because this is a putative class action, and the class Estrada seeks to represent includes members in California.

Mr. Estrada respectfully opposes TaskUs's anticipated motion to dismiss. If this Court is inclined to hold a pre-motion conference, Mr. Estrada respectfully requests the conference not be held August 21st and 22nd due to the undersigned's travel.

Sincerely,

/s/ Carter E. Greenbaum

Carter E. Greenbaum